2017 年 7 月 17 日，星期一

Memcached - 关于未及时修复易受攻击服务器的案例

*作者：*Aleksandar Nikolich 和 *David Maynor*。特别感谢 *Nick Biasini* 提供建议。

MEMCACHED - 安全性不高，修复速度不快

最近，一些受瞩目的系统漏洞被利用，引发了几起全球性勒索软件攻击，对很多组织产生了严重影响。这些类型的漏洞先前已得到修复，组织本可以在攻击开始之前予以解决。很多威胁之所以取得成功，在很大程度上是因为组织未能及时有效地应用补丁，本文介绍的只是其中一个最新的案例。在 2016 年年底，Talos 披露了 Memcached 软件平台中的一系列漏洞。公布漏洞后，Talos 一直在监控易受攻击的系统数量以及修复速度。本文将简要概述这些漏洞，并介绍我们在过去六个月内通过广泛的互联网扫描发现的相关漏洞攻击情况。

Memcached 是什么？

Memcached 是一款用于加快动态 Web 应用速度的高性能对象缓存服务器，广泛应用于一些热门互联网网站。它具有两个协议版本，一个为基于 ASCII 的版本，另一个为二进制版本，用于存储和检索任意数据。二进制协议针对规模进行了优化。

它的预期用途是供 Web 应用服务器访问，并且在任何情况下都不应暴露在不受信任的环境中。该服务器的较新版本包括支持基于 SASL 的基本身份验证，但是根据我们的发现，此功能很少使用。

审计和漏洞

去年十月，我们对 Memcached 服务器进行了一项源代码审计，发现了三种略有不同而又具有相似性的漏洞。所有这三种漏洞都是在二进制协议的实施中发现的。前两种漏洞存在于处理增加和更新缓存对象的代码部分，第三种漏洞存在于上述 SASL 身份验证机制中。所有这三种漏洞都是由整数溢出造成，会导致受控的堆缓冲区溢出；同时，由于协议具有可能被滥用于敏感内存泄漏的性质，这极有可能直接引发漏洞攻击。

供应商收到通知后，立即发布了经我们验证完全可以修复相应漏洞的补丁。最新修复版本的公开发布日期为 2016 年 10 月 31 日。分配给此漏洞的 CVE ID 为 CVE-2016-8704，我们的追踪号为 TALOS-2016-0219。在公开发布后，主要的 Linux 发行版很快发布了各自的更新和建议。需要注意的一点是，主要的发行版（Ubuntu、Fedora…）发布了向后移植的补丁，而未提高服务器的版本号。参考资料：

- http://www.talosintelligence.com/reports/TALOS-2016-0219/
- http://www.talosintelligence.com/reports/TALOS-2016-0220/
- http://www.talosintelligence.com/reports/TALOS-2016-0221/
- https://access.redhat.com/security/cve/cve-2016-8704
- https://www.ubuntu.com/usn/usn-3120-1/

2017 年 1 月的 MongoDB 攻击

说点题外话，在 12 月底/1 月初的某个时候，MongoDB 服务器遭受广泛攻击的消息不胫而走。

MongoDB 是一个驻留在内存中的 NoSQL 数据库。与 memcached 类似，它永远都不应暴露在不受信任的环境中，因此常被开发人员忽略，并且有时候甚至可以通过互联网自由访问生产服务器。

一个众所周知的事实是，成千上万的 MongoDB 服务器都是通过互联网暴露在外，再加上它缺乏任何形式的身份验证或访问控制，所以一些犯罪集团会利用它来牟利。只需几天时间，数以千计的这些可访问 MongoDB 主机便遭到了勒索软件的攻击。

基本上，这些攻击者会连接到服务器，抽取其中所有的数据，并留下说明，要求用特定数量的比特币来赎回这些数据。很快人们发现，多个相互竞争的团伙都在攻击相同的服务器，这使人们确定赎回数据实际上是没有希望的（即使一开始是有希望的）。

媒体广泛报道了这些攻击，毋庸置疑这提高了人们对这一问题的认识，也有望能减少暴露的服务器数量。

Memcached 会面临同样的命运吗？

这场 MongoDB 闹剧让我们不由得思考，如果是 memcached 遭受类似的攻击，会产生怎样的影响。虽然 memcached 不像 MongoDB，它不是一个数据库，但仍然会包含敏感信息，因而服务中断必将进一步导致相关服务中断。此外，我们可以评估所发现漏洞的潜在受攻击面，以及补丁的应用程度。

因此我们决定扫描互联网，了解一下情况…

扫描

要正确获得所需的数据，必须执行一项特殊的扫描。我们需要了解以下几项数据：

- 有多少服务器可以直接通过互联网访问
- 其中有多少服务器易受攻击
- 有多少使用身份验证
- 有多少启用身份验证的服务器仍然易受攻击

我们不能依赖服务器报告的版本，因为如前所述，许多发行版本都发布了向后移植的安全补丁，因此版本字符串并不总能反映补丁应用程度。因此，我们设计了一项特殊测试，通过向服务器发送一个数据包，然后从回复中了解服务器是否易受攻击。

第一系列扫描是在二月下旬执行的。获得第一批数据集后，我们又专门针对已启用身份验证的服务器进行了另一次扫描，这次是在三月初执行的。

扫描结果

我们收集的所有数据大体上都表现出我们预计的结果。逾 10 万台可访问的服务器中，约 80% 仍易受攻击，且仅约 22% 启用了身份验证。有趣的是，启用了身份验证的所有服务器几乎仍然易受我们特别测试的 CVE-2016-8706 的漏洞攻击。具体数据如下：

- 做出有效响应的服务器总数：107786
- 仍易受攻击的服务器总数：85121（约 79%）
- 不易受攻击的服务器总数：22665（约 21%）
- 要求身份验证的服务器总数：23907（约 22%）
- 虽要求身份验证，但易受攻击的服务器总数：23707（约 99%）

按国家/地区细分的数据同样与我们的预计相符：

所有服务器

1. 36937 - 美国
2. 18878 - 中国
3. 5452 - 英国
4. 5314 - 法国
5. 3901 - 俄罗斯
6. 3698 - 德国
7. 3607 - 日本
8. 3464 - 印度
9. 3287 - 荷兰
10. 2443 - 加拿大

易受攻击的服务器

1. 29660 - 美国
2. 16917 - 中国
3. 4713 - 英国
4. 3209 - 法国
5. 3047 - 德国
6. 3003 - 日本
7. 2556 - 荷兰
8. 2460 - 印度
9. 2266 - 俄罗斯
10. 1820 - 中国香港

我们可以从中概括出几个结论。第一，互联网上有大量可轻松访问的 memcached 服务器。第二，不到四分之一的服务器启用了身份验证，其他服务器即使在不存在可利用的远程代码执行漏洞的情况下，也非常容易遭受滥用。第三，人们修复其现有服务器的速度较慢，导致大量服务器有可能遭受攻击者利用我们所报告的漏洞发起的全面攻击。第四，只有少到可忽略不计的一部分服务器启用了身份验证并使用了补丁，因此我们可以得出的结论是系统管理员认为身份验证已能充分应对威胁且补丁不需要更新。所有这四项结论对于组织而言都是不利的。

通知

在完成扫描并得出结论后，我们对所有 IP 地址进行了查询，来获得相关组织的联系人邮箱，以向他们发送通知，简单说明这一情况并提供补救建议。这意味着我们要发送 31000 份唯一性通知邮件。

您好！

我是_____，思科系统公司 Talos Group 的_____。我们注意到，您网络上的一台或多台面向公众的主机运行的 Memcached 实例易受攻击和/或配置错误。

<LIST OF IP ADDRESSES>

易受攻击和配置错误的 Memcached 主机存在重大安全隐患，需要立即引起重视。Talos 之前已经确定了 Memcached 中存在的重大漏洞，这些漏洞可能允许远程攻击者执行任意代码。这意味着这些主机有被恶意威胁实施者入侵并用于其他恶意活动的风险。

有关这些漏洞的详细信息，请查看我们在以下地址发布的博文：
http://blog.talosintelligence.com/2016/10/memcached-vulnerabilities.html

鉴于此问题的严重性，我们强烈建议立即中断这些主机，直到完成修复，因为它们可能会被恶意滥用（例如向用户发送垃圾邮件或盗窃信息）。如果无法立即进行修复，可以禁用二进制协议作为应对某些漏洞的临时应急办法。我们建议您遵循保护 Memcached 主机安全的最佳做法，并确保 Memcached 主机仅限在受信任的环境中可访问。

如果您有任何问题、意见或疑虑，请随时与我们联系：http://www.talosintelligence.com/contact/

顺祝商祺！

<NAME>

二次扫描

在发送通知后，我们在六个月后又进行了一次扫描，以看看这些通知是否产生了任何重大作用。总体结果令人失望，似乎大多数组织都对此通知置若罔闻。如下文所示，只有很小一部

分（约 10%）的系统获得了修复。此外，仍有大量服务器易受攻击，并且未要求身份验证。更令人困扰的是，我们最初发现服务器中有 26% 似乎已不在线，但是我们发现的系统基本还是保持相同的数量。这意味着要么有些系统更改了 IP 地址，要么部署了一大批使用 Memcached 易受攻击版本的新系统。

结果：6 个月后

做出有效响应的服务器总数：106001

仍易受攻击的服务器总数：73403（约 69%）

不易受攻击的服务器总数：32598（约 30%）

要求身份验证的服务器总数：18173（约 17%）

虽要求身份验证，但仍易受攻击的服务器总数：18012（约 99%）

结果：原服务器（107786 个）更新结果

总数：85121

仍然易受攻击的数量：53621

不再易受攻击的数量：2958

不在线：28542（约 26%）

结论

这些类型的漏洞的严重性不容忽视。这些漏洞可能会影响各种大小规模的企业在互联网上部署的平台。就近期蠕虫利用漏洞进行的大量攻击来说，这应该为全世界的管理员敲响警钟。如果置之不理，这些漏洞可能会被利用，对全球组织及其业务产生严重影响。强烈建议立即修复这些系统，以帮助缓解组织面临的风险。

发布者：EDMUND BRUMAGHIN；发布时间：10:35
标签：调查、VULNDEV、漏洞